UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. 5.0096804 BTC, 5,327.090 USDT/ERC20, and 496,452.6472 USDT/TRC20, Defendants.	NO. CV25-611 **VERIFIED COMPLAINT FOR FORFEITURE *IN REM***

I. NATURE OF THE ACTION

1. This is a civil action *in rem* for forfeiture, brought to enforce the provision of 18 U.S.C. § 981(a)(1)(C) for forfeiture of cryptocurrency that constitutes or is derived from proceeds traceable to a violation of specified unlawful activity as defined in 18 U.S.C. § 1956(c)(7), namely, 18 U.S.C. § 1343 (wire fraud).

2. This civil action *in rem* for forfeiture is also brought to enforce the provision of 18 U.S.C. § 981(a)(1)(A) for forfeiture of cryptocurrency involved in a transaction in violation of 18 U.S.C. § 1956 (money laundering) or traceable to such property.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

II. THE PARTIES

3. The plaintiff is the United States of America.

4. On November 8, 2024, U.S. Magistrate Judge Paula L. McCandlis, in the Western District of Washington, issued (i) a seizure warrant ("Seizure Warrant 1") for all contents of Payward Interactive ("Kraken") account number ending in BMYY ("Target Property 1") and (ii) a seizure warrant ("Seizure Warrant 2") for the equivalent value of USDT tokens associated with THVSq4GTzhR9vfEe729LeBBhM3m6TqXhSw ("Target Property 2"). Target Property 1 and Target Property 2 are referred to herein collectively as the "Target Properties". On or about the time these Seizure Warrants were issued, the Target Properties were associated with approximately $883,000 worth of stolen funds (at then applicable conversion rates.

5. On or about November 8, 2024, Internal Revenue Service – Criminal Investigation (IRS-CI) served Seizure Warrant 1 on Kraken. On or about November 15, 2024, Kraken transferred 5.0096804 BTC and 5,327.909 USDT/ERC20 ("Defendant Cryptocurrency 1") to IRS-CI. Defendant Cryptocurrency 1 remains in the secure custody of IRS-CI. As of April 2, 2025, the value of Defendant Cryptocurrency 1 is approximately $416,140.

6. On or about November 9, 2024, IRS-CI served Seizure Warrant 2 on Tether. On or about February 25, 2025, Tether transferred 496,452.6472 USDT/ERC20 ("Defendant Cryptocurrency 2") to IRS-CI. Defendant Cryptocurrency 2 remains in the secure custody of IRS-CI. As of April 2, 2025, the value of Defendant Cryptocurrency 2 is approximately $496,452.

7. Defendant Cryptocurrency 1 and Defendant Cryptocurrency 2 are referred to herein collectively as the "Defendant Cryptocurrency."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

III. JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over an action commenced by the United States under 28 U.S.C. § 1345 and has jurisdiction over an action for forfeiture under 28 U.S.C. §§ 1355(a) and (b).

9. Venue is proper in this district under 28 U.S.C. § 1355(b)(1)(A) because the acts or omissions giving rise to the forfeiture occurred in this district. (Defendant Property was seized in this district).

10. Under Supplemental Admiralty and Maritime Claims Rule G(2)(f), facts in support of a reasonable belief that the United States will be able to meet its burden of proof at trial are as follows and have been verified as set forth in the attached Verification of IRS-CI Special Agent Justin Allen.

11. Under Supplemental Admiralty and Maritime Claims Rule G(3)(b)(i), the Clerk of Court is required to issue a warrant to arrest the Defendant Property if it is in the government's possession, custody, or control. Thus, the Court will have *in rem* jurisdiction over the Defendant Property when the accompanying Warrant of Arrest *in rem* is issued, executed, and returned to the Court.

IV. RELEVANT STATUTES

12. Under 18 U.S.C. § 1343, it is unlawful for anyone, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, to transmit or cause to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

13. Under 18 U.S.C. § 1956(a)(1)(B)(i), it is unlawful to conduct or attempt to conduct a financial transaction, knowing that the property involved in the transaction represents the proceeds of some form of unlawful activity, and which in fact involves the proceeds of specified unlawful activity, knowing that the transaction is designed in whole

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity. This offense is sometimes referred to as concealment money laundering.

14. "Specified unlawful activity," defined in 18 U.S.C. §§ 1956(c)(7) and 1961(1), includes violations of 18 U.S.C. § 1343 (wire fraud), among others.

15. Under 18 U.S.C. § 981(a)(1)(A), any property, real or personal, "involved in" a transaction or attempted transaction in violation of 18 U.S.C. § 1956 (money laundering) is subject to criminal and civil forfeiture. Forfeiture under these statutes applies to more than just the proceeds of the crime. These forfeitures encompass all property "involved in" the crime or the attempted crime, which can include "clean" or "legitimate" money that is commingled with "tainted" money derived from illicit sources. This commingling is a laundering technique that facilitates the scheme because it obfuscates the trail of the illicit funds. *See, e.g.*, *United States v. Huber*, 404 F.3d 1047, 1058 (8th Cir. 2005) (the presence of legitimate funds does not make a money laundering transaction lawful; it is only necessary to show that the transaction involves criminal proceeds).

16. Under 18 U.S.C. § 981(a)(1)(C), "[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to a violation of . . . any offense constituting 'specified unlawful activity'" is subject to civil forfeiture.

V. BACKGROUND RELATED TO CRYPTOCURRENCY

17. **Virtual Currency (or Cryptocurrency):** Virtual currencies are digital tokens of value circulated over the internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies, such as the U.S. dollar, but rather are generated and controlled through computer software. Bitcoin (or BTC) and ether (ETH) are currently the most well-known virtual currencies in use. Other virtual currencies include USDT and TRX.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

18. **Stablecoins:** Stablecoins are a type of virtual currency pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives. For example, USDC is a type of stablecoin pegged to the U.S. dollar. USDC is issued by Circle Internet Financial, LLC ("Circle"). Circle mints USDC tokens and maintains the treasury that backs all USDC on the market.

19. **Tether (USDT):** Tether is a company that manages the smart contracts and the treasury (*i.e.,* the funds held in reserve) for USDT, a stablecoin pegged to the U.S. dollar.

20. **Virtual Currency Address:** Virtual currency addresses are the particular virtual locations to or from which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of letters and numbers.

21. **Private Key:** Each virtual currency address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password, which is needed to access the address. Only the holder(s) of an address's private key can authorize a transfer of virtual currency from that address to another address.

22. **Virtual Currency Wallet:** There are various types of virtual currency wallets, including software wallets, hardware wallets, paper wallets. The virtual currency wallets at issue for the purposes of this affidavit are software wallets (i.e., a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys). A virtual currency wallet allows users to store, send, and receive virtual currencies. A virtual currency wallet can hold many virtual currency addresses at the same time. Wallets hosted by third parties are often called "hosted wallets" because the third party retains a customer's funds until the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

customer is ready to transact with those funds. Conversely, wallets that allow users to exercise total, independent control over their funds are often called "unhosted" wallets.

23. **Blockchain:** The code behind many virtual currencies requires that all transactions involving that virtual currency be publicly recorded on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by a decentralized network of computers, containing an immutable and historical record of every transaction using that blockchain's technology. The blockchain can be updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

24. **Blockchain Explorer:** These explorers are online tools that operate as a blockchain search engine allowing users the ability to search for and review transactional data for any addresses on a particular blockchain. A blockchain explorer is software that uses API and blockchain nodes to draw data from a blockchain and uses a database to arrange and present the data to a user in a searchable format.

25. **Virtual Currency Exchanges (VCEs):** VCEs are trading and/or storage platforms for virtual currencies, such as BTC and ETH. Many VCEs also store their customers' virtual currency in virtual currency wallets. As stated above, these wallets can hold multiple virtual currency addresses associated with a user on a VCE's network. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their customers, including Know Your Customer (or KYC) checks, and to have anti-money laundering programs in place (if they operate and service customers in the United States). VCEs can be centralized (i.e., an entity or organization that facilitates virtual currency trading between parties on a large scale and often resembles traditional asset exchanges like the exchange of stocks) or decentralized (i.e., a peer-to-peer

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

marketplace where transactions occur directly between parties). Kraken is a VCE based in the United States.

26. **Blockchain Analysis:** It is virtually impossible to look at a sole transaction on a blockchain and immediately determine the identity of the individual behind said transaction. That is because blockchain data generally only consists of alphanumeric strings and timestamps. That said, law enforcement can obtain leads regarding the identity of the owner of an address by analyzing blockchain data to figure out whether that same individual is connected to other relevant addresses on the blockchain. To do so, law enforcement can use blockchain explorers, as well as commercial services offered by several different blockchain-analysis companies. These companies analyze virtual currency blockchains and attempt to identify the individuals or groups involved in transactions. "For example, when an organization creates multiple [BTC] addresses, it will often combine its [BTC] addresses into a separate, central [BTC] address (i.e., a 'cluster'). It is possible to identify a 'cluster' of [BTC] addresses held by one organization by analyzing the [BTC] blockchain's transaction history. Open source tools and private software products can be used to analyze a transaction." *United States v. Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020). Through numerous unrelated investigations, law enforcement has found the information provided by these tools to be reliable.

27. **Spoofing and Phishing:** Spoofing is when someone disguises an email address, sender name, phone number, or website URL—often just by changing one letter, symbol, or number—to convince the recipient that they are interacting with a trusted source. Phishing schemes often use spoofing techniques to lure the recipient in, get them to take the bait, and trick them into divulging personal, sensitive information to criminals.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

VI. FRAUD SCHEME AND FINANCIAL TRACING

A. Overview Regarding Theft of Funds from Victim

28. The IRS is investigating a phishing scheme that resulted in the theft of over 1.67 million ERC-20[1] tokens (hereinafter "Victim Tokens") associated with the Victim's virtual currency platform. At the time of the theft, the stolen Victim Tokens were valued at over $6,000,000. The IRS's investigation includes violations of federal wire fraud and money laundering statutes.

29. The victim ("Victim") is a software development company based in Redmond, Washington, that focuses on blockchain-based infrastructure projects. One of the Victim's projects is a blockchain protocol that uses Victim Tokens as the native token for the protocol. Native tokens are used to pay for the computational resources needed for blockchains to operate. The Victim solicited investors to fund their project, and those investors received Victim Tokens from the Victim as part of their investment. Before the theft under investigation here, the Victim was in the process of transferring Victim Tokens to various custodians on behalf of those investors. That process involved investors providing the Victim with virtual currency addresses to which they wanted their Victim Tokens sent.

30. On or about September 25, 2024, an investor ("Investor 1") provided the Victim with an address to which that Investor 1 wanted their Victim Tokens sent. On or about September 30, 2024, the Victim sent a test transfer, consisting of one of the Victim Tokens to the address provided by Investor 1, who then confirmed the transfer. Additionally, the intended custodian of the Victim Tokens was copied on the email.

[1] ERC-20 is a technical standard for establishing fungible assets on the Ethereum blockchain. The rules define (among other things) how ERC-20 assets are transferred within the Ethereum blockchain. ER-20 tokens are sets of fungible digital tokens on the Ethereum network. They are fungible in the sense that each token in the set is indistinguishable from every other token in the set (similar to how one U.S. dollar is indistinguishable from any other U.S. dollar).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

31. Investor 1 was communicating with the Victim from an email address at the domain "iosg.vc." Additionally, the intended custodian copied on that email used an email address at the domain "anchorage.com." As an example, the email address that Investor 1 was using would have been similar to "investor[@]iosg.vc," while the intended custodian's email address would have been similar to "custodian[@]anchorage.com."[2]

32. On or about October 1, 2024, the Victim received an email that the Victim believed was from Investor 1 requesting that the Victim use a different address (the "Attacker Address"), an unhosted address, to receive their Victim Tokens. The content of that October 1 email was identical to the previous September 30 email: it had the same language and signature, and it included the same recipients.

33. But the October 1 email was not in fact from Investor 1. The email was from a nearly identical email address as Investor 1's email, using a common spoofing and phishing technique. The "i" in the email address's domain name was replaced with a lowercase "l." Instead of the email coming from the domain ***i***osg.vc, it came from ***l***osg.vc. As an example, the email address the attacker was communicating would have been similar to investor[@]losg.vc instead of investor[@]iosg.vc. I know from my training and experience that cybercriminals engaged in phishing schemes use such techniques because at first glance the phishing email addresses are easily confused with the real email addresses. Here, the Victim did not notice the difference in the emails and believed that they were still communicating with Investor 1.

34. In that October 1 phishing email, the email address for the intended custodian for the Victim Tokens was also replaced with a phishing domain. The custodian's email address was again copied, but the "g" was replaced with a "q." Thus, instead of the email coming from the domain name anchora***g***e.com it came from

[2] Brackets have been placed around the @ symbols herein to prevent Microsoft Word from automatically converting these example email addresses to hyperlinks.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

anchora*q*e.com. The attacker also replaced the custodian's true email address with a phishing email address: if the true custodian had received the October 1 email, they may have notified the Victim that Investor 1 did not send that email.

35. Both phishing domains, *l*osg.vc and anchora*q*e.com, were registered on or about October 1, 2024, with the same registrar—the same day that the email was sent. The registration's timing is additional evidence of a phishing scheme.

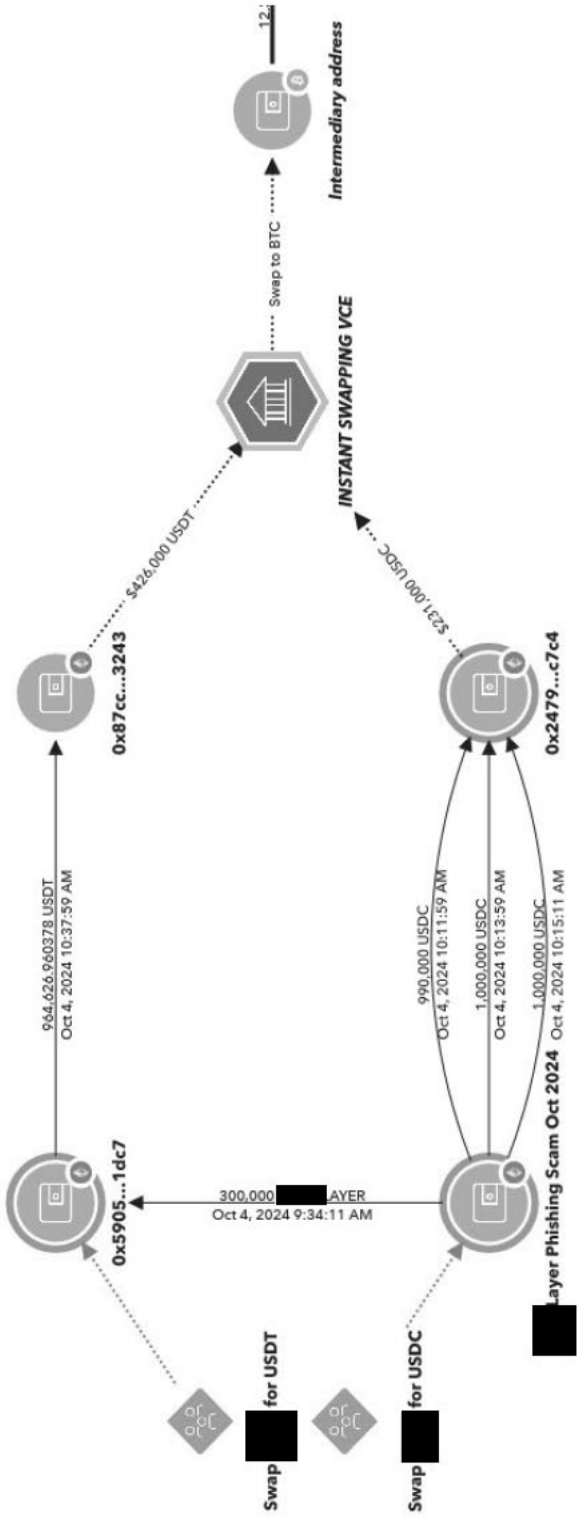
B. Tracing the Trail of the Stolen Funds

36. Just like with the email on or about September 30, 2024, the attackers in the October 1, 2024 email requested a test transfer. On or about October 1, 2024, the Victim completed a test transfer to the Attacker Address. After confirmation from the attacker that they had received the test transfer, the Victim sent 1,673,644 Victim Tokens to the Attacker Address the next day. Approximately two and a half hours after receiving the Victim Tokens, the attacker began converting the Victim Tokens to stablecoins, including USDT and USDC, through a decentralized VCE. Individuals who obtain illicit cryptocurrency often use decentralized VCEs to launder their proceeds to obscure the true origin of the funds.

37. From the decentralized VCE, the attacker(s) further laundered the stolen funds. Throughout October 4, 2024, some of the stolen USDC and USDT were sent to a non-custodial instant swapping VCE and were converted to approximately 15.5 BTC (worth roughly $954,000 at the time of transfer). Non-custodial instant swapping VCEs facilitate the swapping of cryptocurrency (for example, trading USDC for BTC) at very high speeds.[3] Individuals involved in laundering cryptocurrency frequently use these services because they believe there is decreased chance funds will be frozen due to the alleged non-custodial nature. There is a graph below for reference.

[3] Non-custodial instant swapping VCEs claim not to take custody of funds.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

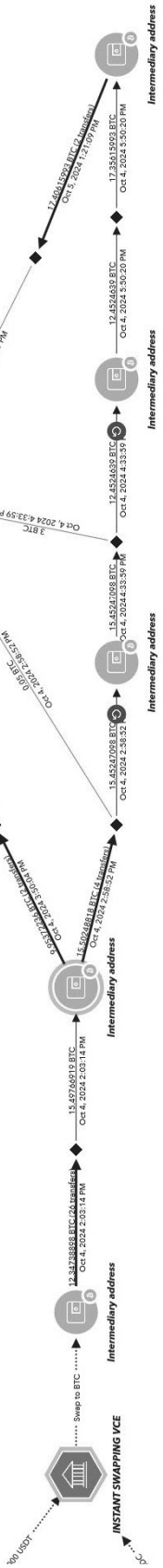
38. The 15.5 BTC was transferred between intermediary addresses in a series of transactions known as a peel chain[4] before being consolidated in Target Property 1 (a VCE account at Kraken). Moving BTC through multiple "hops" before consolidation—such as through a peel chain—is a common method that criminals use to launder the funds by obscuring the control, ownership, source, and purpose of the funds involved in the transfers. The BTC that went to Target Property 1 went through five intermediary addresses before consolidation. The transfers through each intermediary address incurred fees, which could have been avoided if the funds were transferred in a single transaction. There is a graph below for reference.

//

//

[4] A peel chain occurs when a large amount of virtual currency sitting at one address is sent through a series of transactions in which a slightly smaller amount of virtual currency is transferred to a new address each time. In each transaction, some quantity of virtual currency "peel off" the chain to another address (frequently, to be deposited into a VCE), and the remaining balance is transferred to the next address in the chain.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

39. Target Property 1 received four deposits of BTC traceable to stolen funds, three on or about October 4, 2024, totaling approximately 8.05 BTC (worth roughly $487,000 at the time of the transfer) and one on or about October 5, 2024, for approximately 5 BTC (worth roughly $310,000 at the time of the transfer). The first three deposits of BTC to Target Property 1 were converted to USDT on the Tron blockchain within Kraken (i.e., by using Kraken's services to conduct the exchange) and then withdrawn to Target Property 2. The final deposit of BTC to Target Property 1 (for the 5 BTC) was frozen by Kraken and unable to be withdrawn.

40. The timing of these transactions is important. The first of the three transactions on October 4, 2024, to Target Property 1 was for a small amount, 0.05 BTC, commonly referred to as a test transaction. Individuals involved in laundering stolen funds usually perform a test transaction first to see if it is stopped or frozen. Here, each transaction demonstrated the same pattern: a deposit of BTC to Target Property 1, conversion to USDT on the Tron blockchain, and withdrawal to Target Property 2, before the subsequent transaction was initiated. Each transaction was conducted in this manner to reduce the chance that all of the BTC sent Target Property 1 would be frozen and the funds lost if it would have been sent in one large transaction.

41. The investigation revealed that Target Property 1 was created on or about September 23, 2022, and a Danish male's passport was used to authenticate the account. The records also revealed that before the stolen funds were deposited to Target Property 1, it had a balance of approximately $5,332 of USDT,[5] which is far less than the U.S. dollar value of the stolen funds ultimately deposited into Target Property 1 (approximately $797,000 at time of transfer.) As of November 6, 2024, the value of the 5 BTC and the USDT in Target Property 1 was approximately $386,000.

[5] The USDT in Target Property 1 is not traceable to the stolen cryptocurrency. The USDT is nevertheless forfeitable as commingled funds involved in money laundering.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

42. Target Property 2 is an unhosted address on the Tron blockchain. The Tron blockchain uses its native currency, TRX, to pay for the computational resources used to send transactions. Put another way, addresses on the Tron blockchain must contain TRX to withdraw funds because otherwise, there is no way to pay for the fees associated with the transactions.

43. The investigation revealed that Target Property 2's first transaction was a deposit of approximately 1,245 TRX, worth approximately $195 at the time of the transaction,[6] from another non-custodial instant swapping service approximately five minutes before the test transaction from Target Property 1. This TRX was likely deposited in order to pay for subsequent withdrawals of the funds sent from Target Property 1. The contents of Target Property 2 are currently the funds from Target Property 1 and the initial transfer of approximately $195 of TRX. [7] As of November 6, 2024, the total in Target Property 2 was 496,452 USDT (equivalent to $496,717) and 1,245 TRX ($203).

44. At the time the seizure warrants were issued, the combined value of the BTC and USDT in the Target Properties was approximately $883,000.

VII. CLAIM FOR RELIEF

45. As required by Supplemental Rule G(2)(f), the facts set forth in this Verified Complaint support a reasonable belief that the United States will be able to meet its burden of proof at trial. More specifically, there is probable cause to believe that the Defendant Cryptocurrency is subject to forfeiture under 18 U.S.C. § 981(a)(1)(C) because it constitutes or is derived from proceeds traceable to violation of 18 U.S.C. § 1343 (wire fraud). There is also probable cause to believe that the Defendant Cryptocurrency is

[6] Within a few seconds, there was a deposit of 0.000001 TRX (worth less than a fraction of a penny) to Target Property 2.

[7] The United States did not seize the TRX associated with the Target Property 2, as Tether was unable to transfer it. Therefore, whether this TRX is traceable to wire-fraud proceeds is not relevant to this Complaint.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

subject to forfeiture under 18 U.S.C. § 981(a)(1)(A) because it was involved in a transaction in violation of 18 U.S.C. § 1956 (money laundering) or is traceable to such property.

WHEREFORE, the United States respectfully requests:

1. That due notice be given to all interested parties to appear and show cause why the Defendant Cryptocurrency should not be forfeited;

2. That the Defendant Cryptocurrency be forfeited to the United States for disposition according to law; and,

3. For such other and further relief as this Court may deem just and proper.

DATED this 4th day of April, 2025.

Respectfully submitted,

TEAL LUTHY MILLER
Acting United States Attorney

s/Karyn S. Johnson

KARYN S. JOHNSON
Assistant United States Attorney
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101
Phone: 206-553-2462
Fax: 206-553-6934
Karyn.S.Johnson@usdoj.gov

VERIFICATION

I, Justin Allen, am a Special Agent with the Internal Revenue Service – Criminal Investigation (IRS-CI) and have been so employed since 2010. I am currently assigned to the Cyber Crimes Unit in the Washington, D.C. Field Office. I am a law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7). My responsibilities include the investigation of criminal violations of Titles 18, 26, and 31 of the United States Code, and related offenses. As part of my activities, I have been involved in the investigation of different frauds, to include, but not limited to, bank fraud, mail fraud, wire fraud, and tax fraud.

I earned a Bachelor of Science degree in Accounting from Florida State University in 2004 and a Master's Degree in Accounting from Florida State University in 2005. I received my Certified Public Accountant license from the State of Florida in 2006.

I have attended over 500 hours of training in various aspects of criminal investigation as well as classes dealing specifically with tax evasion, money laundering, asset seizure and forfeiture, various financial investigative techniques, and related financial investigations. I received this training from the Federal Law Enforcement Training Center in Glynco, Georgia, as well as the National Criminal Investigation Training Academy for Internal Revenue Service Special Agents, Glynco, Georgia.

In my capacity as a special agent with IRS-CI, I have conducted a variety of financial, tax, narcotics, money laundering, national security, and cybercrime investigations. I have also received training and gained experience in interviewing and interrogation techniques and participated in the execution of federal search warrants involving the search and seizure of computer equipment.

I also have specialized training in cryptocurrencies. This has included training into how publicly viewable "blockchains" record cryptocurrency transactions, how to trace funds through these transactions, attribution techniques used to identify individuals responsible for conducting the transactions, and methods used by individuals to obfuscate

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the source or their control of cryptocurrencies. I have used these techniques in prior and ongoing investigations. Additionally, I have conducted cryptocurrency training for others, both internal to the IRS and for external third parties.

I furnished the investigative facts contained in the foregoing Verified Complaint for Forfeiture *in Rem*. The investigative facts are based on personal knowledge I obtained from my involvement in the underlying investigation, my review of the relevant investigative material, information from other law enforcement officers involved in the investigation, witnesses, other reliable government sources, and my own training and experience.

I hereby verify and declare, under penalty of perjury pursuant to 28 U.S.C. § 1746, that I have read the foregoing Verified Complaint for Forfeiture *in Rem*, that I know its contents, and that the facts it contains are true and correct to the best of my knowledge.

Executed this 4th day of April, 2025.

JUSTIN ALLEN
Special Agent
Internal Revenue Service – Criminal Investigation

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970